INFORMATION - SHARING MODELS

A "LEGAL FOUNDATIONS" SPECIAL STUDY

Report to the
President's Commission
on Critical Infrastructure Protection
1997

This report was prepared for the President's Commission on Critical Infrastructure Protection. The report represents the opinions and conclusions solely of its developer, LegalNetworks, Incorporated. The Commission has not made a judgment on, nor should the publication of this document be taken to represent an endorsement by the Commission for the content of the material contained herein.

Contents

Acknowledgments

The *Legal Foundations* series of reports of the President's Commission on Critical Infrastructure Protection (PCCIP) resulted from the concerted efforts and hard work of several individuals. The Commission gratefully acknowledges Commissioner Stevan D. Mitchell and Assistant General Counsel Elizabeth A. Banker for their leadership and important contributions in developing the *Legal Foundations* series of reports. Their research, writing and analytical contributions were essential to the success of the effort.

The Commission also acknowledges Lee M. Zeichner, Esq. of LegalNet Works Incorporated and his staff, for conceptualizing and maintaining the legal issues database and for providing tireless research support. Finally, the Commission acknowledges the contributions of Senior Consultant Paul Byron Pattak for his deft editing of this compilation.

Preface

Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) and tasked it with assessing the vulnerabilities of, and threats to, eight named critical infrastructures and developing a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required that the PCCIP consider the legal and policy issues raised by efforts to protect the critical infrastructures and propose statutory and regulatory changes necessary to effect any subsequent PCCIP recommendations.

To respond to the legal challenges posed by efforts to protect critical infrastructures, the PCCIP undertook a variety of activities to formulate options and to facilitate eventual implementation of PCCIP recommendations by the Federal government and the private sector. The PCCIP recognized that the process of infrastructure assurance would require cultural and legal change over time. Thus, these activities were undertaken with the expectation that many would continue past the life of the PCCIP itself.

The *Legal Foundations* series of reports attempts to identify and describe many of the legal issues associated with the process of infrastructure assurance. The reports were used by the PCCIP to inform its deliberations. The series consists of 12 reports:

1. *Legal Foundations: Studies and Conclusions*
2. *The Federal Legal Landscape*
3. *The Regulatory Landscape*
4. *Legal Authorities Database*
5. *Infrastructure Protection Solutions Catalog*
6. *Major Federal Legislation*
7. *Adequacy of Criminal Law and Procedure (Cyber)*
8. *Adequacy of Criminal Law and Procedure (Physical)*
9. *Privacy and the Employer-Employee Relationship*
10. *Legal Impediments to Information Sharing*
11. *Federal Government Model Performance*
12. *Approaches to Cyber Intrusion Response*

and two special studies:

- *Information Sharing Models*
- *Private Intrusion Response*

Legal Foundations: Studies and Conclusions is the overall summary report. It describes the other reports, the methodologies used by the researchers to prepare them, and summarizes the possible approaches and conclusions that were presented to the PCCIP for its consideration. The

series has been sequenced to allow interested readers to study in detail a specific area of interest. However, to fully appreciate the scope of the topics studied and their potential interaction, a review of the entire series is recommended.

Introduction

The following discussion describes and analyzes various approaches to information sharing. Each of the approaches, or models, reflects methods adopted by Federal and state government entities and, in many cases, private companies and institutions.

This discussion is divided into two parts. The first part is a discussion of five basic models of information acquisition and dissemination. Where appropriate and useful, bullet points showing “stovepipes” and “filters” are inserted into the text.

The term *stovepipe* is widely used within the intelligence community and refers to systems of vertically aligned information systems that do not communicate with one another. Information stovepipes control the flow of information relevant to infrastructure assurance, and deliver that information to a broadly diverse (and usually functionally disconnected) grouped of public and private sector users.

Filters control the channeling of information concerning infrastructure assurance. Typically there are two types: jurisdictional and legal. Filters limit the types of information which may be collected and used. Within government, for example, jurisdictional and legal filters channel, or block, the flow of information based on "need to know", Congressional grants of authority, or presidential tasking, such as in Executive Orders.

The second part of this paper is a more thorough discussion of key cross-model issues, such as national security, business proprietary matters, antitrust, and liability for disclosure/failure to disclose. These applications illustrate regimes that both thwart and encourage information sharing across critical infrastructures.

The *Legal Foundations* study *Information-Sharing Models* is the companion volume to the *Legal Foundations* study *Legal Impediments to Information Sharing*. The two documents should be studied together to fully understand the issue of information sharing. *Information-Sharing Models* details the current approaches to information sharing and sets the stage for further understanding the concepts described in *Legal Impediments to Information Sharing*.

Part One

Models Of Information Acquisition And Dissemination[1]

Information Clearinghouse Model

Information clearinghouses exist in a variety of forms. Some are administered by Federal agencies, under authorization from statute, regulation or executive order, while others are administered by private entities such as trade associations. There are clearinghouses that are exclusively for information sharing between entities at different government levels, such as between:

- Federal entities,
- Federal and state entities,
- Private entities,
- Federal and private entities, and
- All levels of government—including the municipal level—and the private sector.

The information clearinghouse model includes different methods for gathering information. Some provide for voluntary participation and provision of information, while others are mandatory, requiring that specific public and private entities provide information.

There are also differences in the methods for dissemination of information. Some clearinghouses serve as repositories of information where requesting parties can find information, while others are required actively to distribute information. Additionally, some clearinghouses provide for wider access to information by non-participating parties than others.

Despite these differences, the hallmarks of an information clearinghouse are centralized collection and organization and widespread dissemination of information to participating parties.

[1] These information-sharing models reflect the research of Mitchell Baxter, Esq. and Lee M. Zeichner, Esq. of LegalNetworks, Incorporated, a Washington DC consulting company.

This is distinct from other models which, while providing for the collection and dissemination of information, more severely limit the release of information to parties providing the information.

Applications of The Clearinghouse Model

Department of Commerce Information Clearinghouse

This clearinghouse was established by Congress through 15 United States Code Sections 1151-1157. The stated purpose of the statute is to "make the results of technological research and development more readily available to industry and business, and to the general public," through a "central clearinghouse for technical information which is useful to industry and business." *15 U.S.C. 1151*. Congress directs the Secretary of Commerce to "establish and maintain…a clearinghouse for the collection and dissemination of scientific, technical, and engineering information." *15 U.S.C. 1152*.

Congress further directs the Commerce Department to "search for, collect…and catalog…and to make such information available to industry and business, to State and local governments, to other agencies of the Federal government, and to the general public." *15 U.S.C. 1152(a).* Additionally, the Secretary is directed to effect…the removal of restrictions on the dissemination of scientific and technical data where considerations of national security permit the release of such data to industry and business." *15 U.S.C. 1152(c).*

This information clearinghouse is administered by a Federal agency, the Department of Commerce; information is collected on a voluntary basis, and made available to all interested parties, and on an equal basis. The only restrictions placed on dissemination of information relate to national security matters and other confidential matters such as business proprietary information and trade secrets.

***Information is created and communicated between*:**
Federal government to Federal government,
State government entities, and the private sector.

Information Clearinghouse: Collect and Disseminate Information to All Interested Institutions and Parties. Prevent Dissemination of Classified Information and Trade Secrets, or Information Designated by Private Entities as Business Proprietary Information.

- **STOVEPIPE: Department must refer all relevant technical information to the heads of other government agencies and the military where such information would be useful. *15 U.S.C. 1154*.**

FILTERS: National Security and business proprietary/trade secrets

National Crime Information Center (NCIC)

Congress instructs the Attorney General to "acquire, preserve, and exchange identification records and information" relating to criminal identification and other information which would assist in identifying related matters. *28 U.S.C. 534*. Regulations written pursuant to this statute create a detailed information-sharing system in response to the Congressional mandate. According to 28 Code of Federal Regulations 20.31, "the Federal Bureau of Investigation shall operate the…computerized information system…to link local, state and Federal criminal justice agencies for the purpose of exchanging NCIC-related information,…which includes information in the Computerized Criminal History (CCH) File, a cooperative Federal-State program for the interstate exchange of criminal history record information."

***Information is created and communicated between*:**
Federal government to Federal government,
State government entities, and the private sector.

Information Clearinghouse: Collect and Disseminate Information to Authorized Parties in Government and the Private Sector.

STOVEPIPE: Congress instructs the Attorney General to exchange such information with authorized officials of the Federal Government, the States, cities, penal institutions and other institutions -- which include entities as diverse as railroad police departments and private college and university police departments. *28 U.S.C. 534(a)(4)*.

National Driver Register

This information clearinghouse, under the supervision of the Secretary of Transportation, was established by Act of Congress, under 49 United States Code Chapter 303. The purpose is "to assist chief driver licensing officials of participating States in exchanging information about the motor vehicle driving records of individuals." 49 *U.S.C. 30302(a).* Participation in the program is voluntary, and States may opt in or out at their own discretion. 49 *U.S.C. 30303, 23 C.F.R. 1327.5.*

Access to the information is limited to:

- "Chief Driver Licensing Officials" of participating States
- The Chairman of the National Transportation Safety Board
- The Administrator of the Federal Highway Administration in furtherance of accident investigation[2]
- The individual himself or herself[3].

The individual may also request that the information be disclosed to third parties, such as the Federal Aviation Administration, if the individual is seeking an airman's certificate, or to the Secretary of Transportation, if the individual is seeking employment as a locomotive operator. *See e.g., 49 C.F.R. Pt. 240* (requiring each person seeking certification as a locomotive operator to request that a check of the NDR be conducted, and the results forwarded to his employer.)

Significantly, only these entities may obtain information from the clearinghouse. Thus, information in the clearinghouse is specifically exempted from FOIA disclosure. *49 U.S.C. 30305(c).* Further, insurance companies must use other routes to gain access to this data – such as through state legal regimes and clearinghouses. There are criminal penalties for "unauthorized disclosure and receipt" of clearinghouse data. *49 U.S.C. 30307(a).*

Note that participation in this information clearinghouse is voluntary, while dissemination of the information is restricted. Contrast this structure with that of the following one, which, while apparently similar, contains significant differences.

[2] The National Highway Traffic Safety Administration is administering the fully-electronic register system. *23 C.F.R. 1325.1-1325.4.*

[3] 49 *U.S.C. 30305*.

***Information is created and communicated between*:**
State government and voluntarily sent to the Federal government.
Federal government and provided to designated State government officials and specified Federal government agencies.
Private persons that request information from Federal government Clearinghouse.
Note: Criminal sanctions for unauthorized access and use of information.

Information Clearinghouse: Collect and Disseminate Information to Authorized Parties in Government and the Private Sector.

- **STOVEPIPE: The National Driver Register channels information to qualifying State and Federal departments and agencies. *23 C.F.R. Pt 1327.***
- **FILTER: Access is limited to chief licensing officials of States, and select officials of the NTSB, Federal Highway Administration, and the individual. *49 U.S.C. 30305***

National Motor Vehicle Title Information System

This information clearinghouse is also established by Act of Congress, pursuant to 49 U.S.C. Chapter 305. Unlike the National Driver Registry, which is administered by the Department of Transportation, this information clearinghouse is supervised by the Attorney General. The purpose of the regime is to provide individuals and entities instant and reliable access to information maintained by the States related to automobile titling. *49 U.S.C. 30502.* Information includes validity of titling documents, whether an automobile bearing a particular vehicle identification number has ever been junked, or salvaged, and odometer disclosures. *Id.*

Congress requires all States to participate in this information clearinghouse -- in stark contrast to Congress' mandate in the National Driver Register, which offers States a choice. *49 U.S.C. 30503*. Additionally, there are reporting requirements which obligate private sector owner/operators – such as junk yard owners, salvage yard operators, and insurance carriers—to provide information to the information clearinghouse.[4]

Access to information is much broader than the National Driver Registry. States, law enforcement officials, prospective automobile purchasers, and insurance companies all have access to the information. *49 U.S.C. 30502(e).*

[4] Owner/operators must file monthly inventory reports on junked and salvaged vehicles. See *49 U.S.C. 30504.*

***Information is created and communicated between*:**

State government and sent to the Federal government; participation is mandatory. Federal government and provided to State government officials and Federal government agencies.
Note: Private persons and corporations may obtain information from the Federal government clearinghouse.

Information Clearinghouse: Collect and Disseminate Information to Parties in Federal, State and Local Governments; Private Sector May Also Obtain Information.

STOVEPIPE: Information Clearinghouse channels information to all levels of government and the private sector.

Environmental Protection Agency Solid Waste Information System

The Administrator of the EPA is directed by 42 U.S.C. 6983 to collect and disseminate information relating to methods, costs and management practices for the collection, disposal, financing and reduction of solid waste. The statute further calls for the establishment of a central reference library, and the development of model accounting systems and codes. *Id.*

Pursuant to Federal legislation, Congress directed the EPA to implement information programs "for the rapid dissemination of information on solid waste management…including the results of any relevant research, investigations…studies, or other information which may be useful," and "educational programs to promote citizen understanding of the need for environmentally sound…practices." *42 U.S.C. 6983(e).*

There are close to 100 information clearinghouse models at the Federal, state, and local government level.

Advisory Committee/Commission Model

Federal and State government committees and commissions are a common form of information collection and dissemination in the United States. Some are established to study one issue or set of issues, and then disband (e.g. the President's Commission on Critical Infrastructure Protection (PCCIP)), while others are established and charged with a continuing mission. There are commissions that deal only with information sharing within a particular Federal department or agency, some within the entire Federal government, and some which are concerned with relationships between Federal departments and agencies and their State counterparts.

The distinguishing feature of this model is a centralized body which gathers information and works in a collaborative manner to coordinate collection, analysis, and dissemination of the information; these entities also resolve specific issues, which, at least in part, define the committee or agency's mission or purpose.

Applications of the Advisory Committee/Commission Model

Interagency Security Committee (ISC)

Established by Executive Order 12977, the ISC is intended to:

> *"enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by Federal employees for nonmilitary activities, and to provide a permanent body to address continuing government-wide security for Federal facilities. Executive Order 12977."*

The committee is comprised of representatives of all Federal departments, plus representatives from several Federal law enforcement agencies.

In addition to establishing security policies and strategies, the Committee is charged with:

1. encouraging agencies with security responsibilities to share security-related intelligence in a timely and cooperative manner (*E.O. 12977 Sec 4(A)),* and

2. assisting in "developing and maintaining a centralized security database of all Federal facilities." *Id. Sec. 4(E).*

The Executive Order mandates compliance—that is, all relevant agencies must share the information. The President also requires all relevant agencies to comply and cooperate with the Committee's policies and recommendation, except where the Director of Central Intelligence determines that compliance would jeopardize intelligence sources and methods. *Id. at Sec. 6(b).*

***Information is created and communicated between*:**
Federal government to Federal government.

Note: Federal government agencies required to provide information to a committee, which collects, analyzes, and disseminates the information within the Federal government.

- **STOVEPIPE: Security-related intelligence is to be shared between all members of the committee and ultimately, after analysis, to specific government agencies and entities.**

- **FILTER: Classified, National Security Information.**

Advisory Committee for Trade Policy and Negotiation

Some committees collect specific and specialized information from the private sector; the information is then used, in conjunction with information collected by the Federal government to address an issue, or series of issues. As part of the Trade Act of 1974, 19 U.S.C. 2111 et seq., Congress provides that "the President shall seek information and advice from representative elements of the private sector and the non-Federal governmental sector with respect to...negotiating objectives, bargaining positions...and the operation of any trade agreement," as well as other trade policy matters. *19 U.S.C. 2155(a).*

Congress further directs the President to establish an advisory committee, to provide overall policy advice on such matters. *19 U.S.C.2155(b).* The committee is to be made up of representatives of non-Federal government, labor, industry, agriculture, small business, service industries, retailers and consumer interests. The U.S. Trade Representative is directed to make available to the committee such information and resources as it requires. *19 U.S.C. 2155(c).*[5]

***Information is created and communicated between*:**

Private Sector to Federal Government.

Note: Federal Government Required to Collect Specialized Information from Cross-Section of Private Sector; Information used by Executive Branch.

- **STOVEPIPE: Information in separate, private sector stovepipes transferred to Federal government. (e.g., specialized knowledge on an industry's trade-related knowledge provided to USTR; USTR assists in information collection).**

Advisory Committee on Intergovernmental Relations

This committee is established by 42 U.S.C. 4272, in order to "strengthen the ability of the United States federal system of government to meet the problems of an increasingly complex society by promoting greater cooperation, understanding and coordination of activities between the separate levels of government." *5 C.F.R. 1701.3*

Two of the primary objectives are

1. "[b]ringing together representatives of the Federal, State and local governments for the consideration of common problems, and

2. [p]roviding a forum for discussing the administration and coordination of Federal grant and other programs requiring intergovernmental cooperation." *Id.*

Information resources include a wide range of private sector and Federal, state, and local government representatives. The committee is composed of 26 members, six appointed by the President, (three from the executive branch and three private citizens), three Senators appointed by the President of the Senate, and three Members of Congress appointed by the Speaker of the

[5] The Act additionally provides for the establishment of individual general policy committees, at the President's option. *Id.*

House of Representatives. The remaining four Governors, three members of State legislative bodies, four mayors, and three elected county officials are all appointed by the President. *5 C.F.R. 1701.4.*

To ensure that the committee does not become a political vehicle, designators to the committee are required to appoint bipartisan membership. *5 C.F.R. 1701.5.*

***Information is created and communicated between*:**

Private Sector and Federal, State, And Local Government
***Note: Shared And Analyzed, And Ultimately Offered To All Levels Of Government And The Private Sector*.**

A Plethora of Advisory Committees - Federal Advisory Committee Act, S 2, 5 U.S.C.A. App. 2:

(a) The Congress finds that there are numerous committees, boards, commissions, councils, and similar groups which have been established to advise officers and agencies in the executive branch of the Federal Government and that they are frequently a useful and beneficial means of furnishing expert advice, ideas, and diverse opinions to the Federal Government.
(b) The Congress further finds and declares that--
- **(1) the need for many existing advisory committees has not been adequately reviewed;**
- **(2) new advisory committees should be established only when they are determined to be essential and their number should be kept to the minimum necessary;**
- **(3) advisory committees should be terminated when they are no longer carrying out the purposes for which they were established;**

Mandatory Exchange Or Provision Of Information Model

Under this model, one entity is required, through a variety of legal mechanisms, to provide information to another entity. The distinguishing characteristic of this model is that the collecting entity is generally under no obligation to disseminate the information— except to related or supervisory agents.

In some cases, there is a statutory requirement that one party give information of a certain type to another party. In other cases, an agency or department is given subpoena power to compel production of information, testimonial or documentary, from another entity or individual.

Federal Subpoena Authority

Typically, Federal departments and agencies are given subpoena power to gather information in furtherance of their statutory missions. Several common examples include:

- **The Federal Communications Commission** (FCC) has "the power to require by subpoena the attendance and testimony of witnesses and the production of all books, papers, schedules of charges, contracts, agreements, and documents relating to any matter under investigation." 47 U.S.C. 409(e). The regulations relating to the issuance of subpoenas by the FCC, which outline in great detail how the legal mechanism operates, are found at 47 C.F.R. 1.331.

- **The U.S. International Trade Commission**[6] (ITC) is given extensive powers to gain access to information pertinent to its investigations. The Tariff Act of 1930 provides that the Commission has "the right to copy any document, paper or record, pertinent to the subject matter under investigation, in the possession of any person, firm...or association engaged in the production, importation or distribution of any article under investigation...may summon witnesses...may require any [party] to produce books or papers...and...to furnish in writing in such detail and in such form as the Commission may prescribe, information in their possession pertaining to such investigation." 19 U.S.C. 1333.

- To facilitate the collection of relevant information from private entities, including non-US industries and corporations, the ITC has extensive rules governing the collection of Business Proprietary Information. See 19 C.F.R. 207.7 (1997) Under this regime, parties may submit sensitive business information (trade secrets) to the Commission and attorneys involved in the case. These regulations carry severe sanctions for lawyers, and other consultants, who divulge business proprietary information -- even if by mistake. Penalties include disbarment (19 C.F.R. 207.7(d), (e)) and referrals to the US attorney for further prosecution and publishing violators names in the Federal Register.

- **The Secretary of Transportation** is given similar power to subpoena witnesses and records related to a proceeding or investigation pursuant to 49 U.S.C. 502 (d), and 49 U.S.C. 13301.

Private Subpoena Authority

The Federal Rules of Civil Procedure provide a mechanism for private litigants to compel the production of witness testimony, and documentary evidence, and written answers to interrogatories. The general discovery provision is Rule 26; the authority to issue subpoenas is found in Rule 45.

[6] Trade-related investigations often involve the ITC and the International Trade Administration ("ITA"), under the Department of Commerce. The ITA has similar rules and regulations for collection of business proprietary information – including sanctions for the release of that information. *See* 19 C.F.R. 353 et seq.

Reports, Disclosures and Notification

In some instances, a party is given a statutory mandate to provide certain information to another party, either with or without the need for a request.

- In the statute providing for the powers and duties of the Inspector General of the Department of Energy, Congress requires that "the Inspector General shall report expeditiously to the Attorney General whenever the Inspector General has reasonable grounds to believe there has been a violation of Federal criminal law. *42 U.S.C. 7138(j)*.

- Under the Tariff Act of 1930, at 19 U.S.C. 1332(g), Congress specifies that the U.S. International Trade Commission "shall put at the disposal of the President…the Committee on Ways and Means of the House of Representatives, and the Committee on Finance of the Senate, whenever requested, all information at its command, and shall make such investigations and reports as may be requested by the President or by either of said committees or by either branch of Congress."

- Executive Order 10450, which concerns security requirements for government employment, mandates that "[w]whenever there is developed or received by any department or agency indicating that the retention of employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency."

Cooperation With Other Agencies

Listed below are two of many examples in which Congress or the President, via Executive Order, mandates information sharing:

- Congress, at 19 U.S.C. 1334, requires the ITC to "act in conjunction and cooperation with the Treasury Department, the Department of Commerce, the Federal Trade Commission, or any other departments, or independent establishments of the Government, and that such [entities] shall cooperate fully with the Commission…and, when directed by the President, shall furnish to the Commission, on its request, all…information in their possession relating to any of the subjects of investigation by the Commission.

- Executive Order 12333, which concerns national security coordination, mandates that the heads of all Executive Branch departments and agencies shall give the Director of Central Intelligence access to all information relevant to national intelligence needs.

Voluntary Cooperation Or Exchange Of Information Model

Under this model, one entity exchanges information even in the absence of a Congressional or Presidential mandate. The exchange can take place pursuant to statutory *authorization* to communicate, through an organizational structure that facilitates such information exchange, or on an informal basis. The statutory exchanges tend to involve those between Federal agencies, or Federal and State agencies. Private exchanges tend to occur through organizations such as trade associations, or through informal channels, such as a private industry or through individual, private sector contacts.

Applications of the Voluntary Cooperation or Exchange of Information Model

Emergency Federal Law Enforcement Assistance (EFLEA)

This law was enacted to give States a means to request Federal law enforcement assistance in the event of an emergency:

> *"an uncommon situation which requires law enforcement, which is or threatens to become of serious or epidemic proportions, and with respect to which State and local resources are inadequate to protect the lives and property of citizens or to enforce the criminal law." 42 U.S.C. 10502(3).*

Assistance means funds, equipment, training, *intelligence information*, and personnel. *See 42 U.S.C. 10502(1).*

Under EFLEA, Congress offers a mechanism for States to apply to the Attorney General for such information. The Attorney General then may approve or disapprove the application, based on certain criteria specified in the statute, such as the nature of the emergency, availability of resources, cost, and various federalism issues. *42 U.S.C. 10501*.

Attorney General Seeking State or Local Assistance

When the Attorney General or President determines that an immigration emergency exists, and State or local assistance is required, Department of Justice regulations provide a mechanism for such a request and exchange of information. *See 28 C.F.R. 65.84.* Under the regulations, the Attorney General is authorized to negotiate the terms and conditions of the assistance with the State or local government, and funds can be provided by a reimbursement agreement, grant or cooperative agreement.

In exigent circumstances, the Attorney General is authorized to seek State or local assistance and agree to provide funding without a written agreement. *28 C.F.R. 65.84(c).*

Secretary of Transportation Cooperating With States

In carrying out his responsibilities under the general authority enabling statute, 49 U.S.C. 502(c), the Secretary of Transportation may:

(1) confer and hold joint hearings with State authorities;

(2) cooperate with and *use the services, records,* and facilities of State authorities; and

(3) make cooperative agreements with a State to enforce the safety laws and regulations of a State and the United States related to highway transportation.

These arrangements include the all information held by the State government relating to safety laws and highway transportation.

Exchange of Information Through Organizations

Most industries and private sector interest areas have trade associations and other organizations established for the purpose of representing their interests as a whole before Congress and the individual State legislatures, and Federal and State executive agencies and Courts. These organizations typically provide for the sharing and exchange of information, such as through newsletters, journals, and other publications, trade practice groups and conferences.

In their role as lobbyists and advocates, these organizations also serve as a major conduit for information flowing from the private sector to Federal, State and local governments.

Informal Exchanges of Information

In the private sector, an individual or group at one company may simply contact a counterpart at a different company to discuss a matter relevant to both companies, or even to all companies in a particular industry segment.

There are many reasons that private companies would need to exchange information, as opposed to using a third-party intermediaries. If a security breach or attempt is discovered, for example, it is important that one company be able to immediately warn other companies facing the same risk. It also allows companies which may have incomplete information about a security threat or criminal activity to combine information resources.

Cyber-related breaches offer the most obvious example. Where such breaches raise public relations issues, companies are especially sensitive to government information exchange requests, for fear of loss of control and publicity. Under these circumstances, information exchanges between company Systems Administrators and Operators may solve problems for the future and offer both companies an opportunity to pool resources without adverse publicity.

Note, however, that these private exchanges of information—including those discussed in numbers 3 and 4 above -- may give rise to Federal and state antitrust violations. We discuss these antitrust issues more fully under the Cross-Model Issues, discussed below.

Summary

Voluntary Cooperation or Exchange of Information Model

Federal, State, and local governments exchange information on a voluntary basis. Private sector similarly exchanges information with other private entities.

Threat And Hazard Detection And Notification Model

This model is, in one sense, a combination of the information clearinghouse and mandatory notification models, with the additional requirement that the collector of the information must then disseminate the information through specific channels or to specific parties; these parties may are granted the right to receive the information.

There are several levels of notification, ranging from simple and unsophisticated models (*e.g.*, sending notices to be posted on a wall) to more complex, expensive, and far reaching (*e.g.*, issuing general public announcements or extensive notification campaigns which require contacting all individual members of a particular group).

Applications of the Threat and Hazard Detection and Notification Model

Emergency Planning and Right-to-Know

This multi-tiered structure of State and local planning districts and emergency response committees is established by 42 U.S.C. Chapter 116. Under this system, each local entity is required to evaluate potential hazards, available resources, and appropriate responses to various emergencies. *42 U.S.C. 11003.* A national response team is established to review each local committee's plans, as well as to issue guidance documents to assist in the preparation of emergency plans. *42 U.S.C. 11003(e), (f), (g).*

Additionally, the operator of any facility determined to be relevant to the plan, by virtue of its production, use or storage of hazardous materials, is required to designate a representative to participate in the planning process, and to provide information as requested by the committee. *42 U.S.C. 11003(d).*

In the event of the release of "an extremely hazardous substance referred to in [the Act], " from a facility, the operator of the facility is required to provide immediate notice to the community and State emergency planning officials. *42 U.S.C. 11004.*

- STOVEPIPE: Facility operator required to provide information to committee, and to notify planning officials in the event of a release.
- FILTER: Trade secrets are protected from public disclosure. *42 U.S.C. 11042.*

Natural Oil and Hazardous Substances Pollution Contingency Plan

This plan, codified at 40 C.F.R. 300, shows a fully developed example of this type of model. It provides for the establishment of a National Response Team, *40 C.F.R. 300.110*, and Regional Response Team, *15 C.F.R. 300.115*, which are to coordinate and share information in the preparation of contingency plans. *40 C.F.R. 300.205*.

Industry groups and academic organizations are encouraged to participate in planning, committing resources, and sharing technical and scientific information; the Scientific Support Coordinator is authorized to act as a liaison between the On Scene Coordinator and the Regional Project Manager, and all interested organizations. *40 C.F.R. 300.185*.

In essence, this is an information clearinghouse within the threat and hazard detection and notification model.

There are notification requirements and a permanent infrastructure is established and continuously manned for handling emergency responses. *40 C.F.R. 300.125.* A chain of command is established, and provision is made for down-line and lateral communication of information.

Finally, recognizing that "it is imperative to give the public prompt, accurate information on the nature of the incident and the actions underway to mitigate the damage," Section 300.155 calls for the establishment of a Joint Information Center to coordinate the collection and dissemination of information through appropriate media and other channels. [Again, a clearinghouse is established within this model.]

The following two examples highlight the differences in notification required, both in the form and the breadth of notification required.

FDA Consumer Right-to-Know About Pesticide Chemical Residue

As part of a larger statute requiring the establishment of standards regarding tolerance of pesticide residues, which is found at 21 U.S.C. 346a, there is a provision regarding public disclosure and notification of the findings of such research. *21 U.S.C. 346a(o).* This section provides that the Administrator of the Food and Drug Administration, in consultation with the Secretaries of Agriculture and Health and Human Services, "shall publish in a format understandable to a lay person, and distribute to large retail grocers for public display (in a manner determined by the grocer), … a discussion of the risks and benefits of pesticide chemical residues in or on food," and other specific information about chemical pesticide residues which may be useful to consumers. *Id.*

- FILTER: Confidential business information is protected from disclosure. *21 U.S.C. 346a(I).*

This provision, which calls for a narrow scope of notification, should be contrasted with the following one, which calls for a much broader scope of notification.

Consumer Product Safety Commission Remedies Respecting Banned Hazardous Substances

15 U.S.C. 1274(a) provides that, "[i]f any article or substance…is defined as a banned hazardous substance,…and the Commission determines…that notification is required to adequately protect the public…the Commission may order the manufacturer or any distributor or dealer…to take any one or more of the following actions:

(1) To give public notice that the article or substance is a banned hazardous substance.
(2) To mail such notice to each person who is a manufacturer, distributor, or dealer of such article or substance.
(3) To mail such notice to every person to whom the person giving the notice knows such article or substance was delivered or sold."

Additionally, the Commission has the power to order repairs and changes to be made, or for recalls of the article or substance. *15 U.S.C. 1274(b).*

Note: The latter two examples are relevant to infrastructure assurance in that they go to the questions of the form of notification of hazard utilized, and the breadth of "audience" the notification is required to reach. The FDA provision calls for posters to be mailed to large grocers, omitting smaller grocery chains, in addition to "mom-and-pop" grocery stores, while the CPSC provision requires public announcements <u>plus</u> individual notification of <u>every</u> party who may be affected.

This issue is more fully discussed in the Cross-Model Issues Section of this discussion, under the subheading "Liability for Failure to Disclose or Inform."

Part Two

Cross-Model Issues

There are a number of issues which are relevant to many, if not all of the models. These issues will be discussed in this section, with reference to particular models as necessary. In one sense, the issues may be referred to as "stovepipes" and "filters."[7]

Stovepipes & Filters -
Limiting the Flow of Information to the Necessary Parties

- Stovepipes - In all of these issues, as well in all of the models, the "stovepipe" issues involve the following inquiries:

  (1) Who gets access to information?
  (2) Who provides access to information?
  (3) Who must be informed?
  (4) Who may be informed?

- Filters - In all of these issues, as well as in all of the models, the "filter" issues raise the following inquiries:

  (1) What mechanisms cause information to be withheld?
  (2) Who is responsible for withholding information?
  (3) What liability is there for filter "breaches?"

[7] See definitions in introduction of this discussion.

National Security

This discussion will be limited to key statutes and executive orders which highlight how national security rules affect the flow of information within and outside of government channels.

- STOVEPIPES AND FILTERS: The entire national security infrastructure is a study in stovepipes and filters: who gets access and what information is withheld from disclosure.

The National Security Infrastructure

The general statute for the establishment and structure of the national security infrastructure is 50 U.S.C. Chapter 15. Coordination for national security is discussed beginning at *50 U.S.C. 402,* which establishes the National Security Council and the Central Intelligence Agency. Protection of the operational files of the CIA is provided for at *50 U.S.C. 431,* which exempts from disclosure under *5 U.S.C. 552a* those files which document intelligence or counterintelligence operations or arrangements, means of collection, or sources.

50 U.S.C. 435 establishes the requirement that no employee of the executive branch, except as permitted by the President, may be given access to classified information without an appropriate background check.

Classifying, Safeguarding and Declassifying Information

Executive Order 12958 "prescribes a uniform system for classifying, safeguarding and declassifying national security information." The Implementing Directive for the Order is found at *28 C.F.R. 2001.* Each department and agency of the Federal Government has promulgated rules pursuant to this Order. For example, the Department of Transportation rules are found at 49 C.F.R. Part 8, the Department of Justice rules are found at 28 C.F.R. Part 17, and FERC rules are found at 18 C.F.R. Part 3a.

Information Sharing

Executive Order 12333 provides that the agencies within the intelligence community, in addition to participating in intelligence activities, shall "ensure the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information, and products."

Liability for Disclosure of Classified Information

There are numerous statutes sanctioning – with criminal penalties -- the disclosure of classified information. For example, 18 U.S.C. 798, which is part of the chapter relating to espionage and censorship, provides that "[w]hosoever knowingly and willingly communicates...to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interests of the United States...any classified information" relating to codes, ciphers or communication intelligence activities, is subject to a fine, prison term, and forfeiture of assets derived as a result of, and used in the facilitation of the violation.

"Foreign" Person - Corporate Access to Confidential Information

A major area of concern is how to determine to which entities it is in the national interest to disclose sensitive information. Many key infrastructure-related companies may not be entirely American-owned. What exactly is a "foreign" company? The answer to this question is not entirely clear.

Even Congress has expressed uncertainty over the concept, as evidenced by a hearing held on November 1, 1989 by the House of Representatives Subcommittee on Science, Research and Technology and the Subcommittee of International Scientific Cooperation. The subject of the hearing was "*What Is A U.S. Company?"* The purpose of the hearing was to identify the guidelines under which foreign owned and U.S. based multinational corporations should be allowed to participate in Federally-funded research projects, consortia, or joint ventures.

Various agencies have defined "foreign" differently for their own purposes. For example, the Department of Energy has established a set of sophisticated guidelines for determining the level of foreign interest, ownership, control, or influence over a government contractor. These guidelines, which are codified at 48 C.F.R. 952.204-73, contain a series of questions that draw on similar rules in several legal regimes, including customs, tax, and securities regulation.

Department of Energy Listing of Foreign Interest and Ownership Questions

Several Questions include:

- Does a foreign interest own or have a beneficial ownership interest in five percent or more of your organization's voting securities?
- Identify the class of shares issued which are owned by foreign interests, listed by country.
- Does your organization own ten percent or more of any foreign interest? Supply the particulars.
- Does any foreign interest have management positions such as directors, officers, or executive personnel in your organization? Provide particulars.
- Does any foreign interest control or influence, or is any foreign interest in any position to control or influence the election, appointment, or tenure of any of your directors, officers, or executive personnel? Identify and discuss.
- Does your organization have any contracts, binding agreements, understandings, or arrangements with foreign interests that cumulatively represent ten percent or more of your organization's gross income? Provide particulars on any intellectual property ties, trade secrets, licensing, patent agreements, cartel or industry ties…
- Is your organization indebted to foreign interests? If include debentures, discuss whether the securities are convertible, etc.
- Does your company derive any income from Communist countries included in Groups Q, S, W, Y, and Z in Supplement No. 1 in 15 C.F.R. part 770 (e.g., Cuba, Syria, North Korea.).

These questions are presented to contractors to determine whether such foreign interest rises to such a level as to pose a security concern and must be certified.

The Internal Revenue Service has its own classification of "controlled foreign corporations" for tax purposes, which is codified at 26 U.S.C. 957. This provision considers a controlled foreign corporation one in which more than 50 percent of the stock is owned by U.S. shareholders.

Access to Classified Information by Non-United States Citizens

Executive Order 12968, Section 2.6 provides that "where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information only for specific programs, projects, contracts…for which there is a need for access." The access is limited to that level which the U.S. Government "has determined may be released to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior 10 years of the subject's life can be appropriately investigated."

Private Sector And Other Confidential Matters

This issue cuts across nearly all of the models, as it is necessary to ensure that information which private companies wish to keep secret remains secret. Without built-in guarantees of such confidentiality, no business would engage in information sharing of any kind with either a government or private entity, unless forced to do so. Even then, the amount, veracity, and breadth of information would likely be limited.

Protective Measures for Trade Secrets and Proprietary Information

Confidential materials are protected through a variety of mechanisms in the public and private sectors. These include such measures as statutes mandating that information received by government agencies in the execution of their statutory missions be held in confidence, restricting access to such information, and providing penalties for the disclosure of such information. There are also judicial (JPOs) and administrative protective orders (APOs) which permit confidential information to be provided to certain parties, such as attorneys, while the information is withheld from other parties, such as their clients.

Examples include:

- The Tariff Act of 1930, at 19 U.S.C. 1677f(b) provides that information submitted to the ITC which is designated as proprietary by the person submitting it, shall not be disclosed to any person outside of those Commission persons who are directly involved in the relevant investigation, or to an officer of the U.S. Customs Service who is conducting an investigation regarding fraud under the Act, without the consent of the person submitting it. The Act further provides for limited disclosure of certain proprietary information under protective order. *19 U.S.C. 1677f(c).*

- By statute codified at 49 U.S.C. 1114, the NTSB may disclose trade secrets only-

(1) to another...instrumentality of the U.S. Government when requested for official use
(2) to a Committee of Congress...having jurisdiction...when requested;
(3) in a judicial proceeding under a court order that preserves the confidentiality of the information without impairing the proceeding; and
(4) to the public to protect health and safety after giving notice to any interested person...and an opportunity for that person to comment...if the delay...would not be detrimental to health and safety.

Balancing Information Disclosure With Other Public Policy Considerations

An interesting feature of this statute is the provision for the protection of the voluntary submission of information to the NTSB. The provision prohibits the release of such information "if the Board finds that the disclosure of the information would inhibit the voluntary provision of that type of information." *49 U.S.C. 1114(b)(3).*

A similar provision, valuing disclosure of information to protective bodies over the release and use of such information by third parties, can be found at 49 U.S.C. 504(f), which states that "[n]o part of a report of an accident occurring in operations of a motor carrier...and required by the Secretary [of Transportation], and no part of an investigation of the accident made by the Secretary, may be admitted into evidence or used in a civil action for damages related to a matter mentioned in the report or investigation."

- The U.S. criminal code has a chapter devoted to the protection of trade secrets, 18 U.S.C. Chapter 90, which has two primary provisions. The first, which is under the heading "Economic Espionage," at 18 U.S.C. 1831, prohibits the theft of trade secrets with the intention of benefiting any foreign entity. Individuals violating this section are subject to be fined up to $500,000 and imprisoned for up to 15 years; organizations face fines up to $10,000,000.

- The second provision, 18 U.S.C. 1832, punishes the theft of a trade secret with the intention of benefiting anyone other than the owner of the trade secret with a fine and imprisonment of up to 10 years. Organizations face fines of up to $5,000,000. The statute also provides for judicial orders to preserve confidentiality of trade secrets in prosecutions under the statute. *18 U.S.C. 1835.*

- There are provisions in the Federal Criminal and Civil Codes for protection of confidential matters which may be uncovered in court proceedings. Federal Rule of Criminal Procedure 6(e) prohibits disclosure by grand jurors and grand jury employees of any matter occurring before the grand jury. Exceptions are made for disclosure to government attorneys, government personnel as deemed necessary by a government attorney, and for a few other disclosures such as other grand juries, or state law enforcement officials under limited circumstances.

- Federal Rules of Civil Procedure 26 and 45, which concern discovery and subpoenas, both contain provisions for the issuance of protective orders to ensure the confidentiality of sensitive information.

Antitrust Liability

There are several antitrust issues which arise in the context of infrastructure information sharing. The mere act of information sharing about security-related matters should not raise questions of antitrust or unfair trade liability, which generally arise in the contexts of price fixing and market splitting. Such questions do arise, however, in the context of exclusion of one or more companies from access to information. In this event, there is a possibility that an excluded company could claim that it is the victim of a boycott, or that it is being denied access to an "essential facility."[8]

[8] An "essential facility" is well defined in antitrust law and includes situations where a person or company denies access to a facility that is necessary to conduct business. Information can also be considered an "essential facility."

While much informal information sharing takes place, many companies remain hesitant to provide even crucial security information to competitors, for fear of antitrust liability.

While such a claim may be brought, it is not clear how likely it would be that such a claim could be successfully prosecuted, civilly or criminally. The standard for establishment of an "essential facility" is high, requiring that the excluded party have no other means for gaining access to, or duplicating the denied facility.

One question that must be factored into this equation is the potential likelihood of this occurring. It would appear to be in the best interests of all companies in a particular industry to either share no information with any other companies, or to cooperate with all companies desirous of ensuring industry-wide security. Nevertheless, the possibility does exist that two or more companies, privately or through the establishment of a restrictive trade organization, might attempt to drive other competitors out of the market by withholding key information.

Liability For Failure To Disclose Or Inform

Duty to Provide Information

1. ***What is the duty of the Federal government to disclose information to owner/operators of a critical infrastructure?***

2. ***What is the duty of an owner/operator of a critical infrastructure to disclose information to***

    - ***Federal government?***
    - ***A different owner/operator? A competitor?***

3. ***Duties arise by operation of law or by contract:***

    - ***Absent a well-defined duty, there is typically no liability for failure to disclose information.***

    - ***Duties may be imposed at the Federal level by the President (Executive Order), Congress (statute), the Courts (court decision);***

    - ***Typically, each State (through the legislature or the courts) addresses***

whether private entities have an affirmative duty to disclose information.

- ***A duty may arise between private parties by contract (e.g., Sprint promises to notify AT&T of any cable break) or by tort law.***

- ***It is well-recognized tort law that one who undertakes to warn the public of a danger and thereby induces reliance must perform his good samaritan task in a careful matter. That is, if you choose to inform, you bear the consequences of informing incorrectly or incompletely.***

Congress, state legislatures and courts have all addressed general duties to act. For critical infrastructure assurance and information-sharing purposes, the affirmative duty to disclose information raises two issues. The first involves liability of the Federal government's failure to disclose information in its possession to a private party. The second involves the liability of a private party for failure to disclose or report information which the party is under a statutory, regulatory, or, potentially, a common law duty to disclose.

The *Federal Torts Claim Act* creates potential liability for the Federal government in dealing with private parties. The possibility exists that a party who has sustained a loss that could have been prevented had certain information been relayed to him will attempt to hold the entity responsible for intentionally or negligently withholding that information. Such a claim could be brought under the Tort Claims Act, which provides that the United States shall be liable in the same manner and to the same extent as a private individual under like circumstances, with many exceptions, including those for pre-judgment interest and punitive damages. *28 U.S.C. 2674*.

There is an additional exception to U.S. liability which is relevant here: 28 U.S.C. 268(a) exempts "any claim based upon an act or omission of an employee of the Government, exercising due care, in the execution of a statute or regulation." The question to be addressed is whether this would bar a claim against the U.S. from an aggrieved party who was omitted from notification of critical security information.

Additionally, many statutes, regulations and executive orders providing for disclosure of certain information have provisions stating that they do not create any right or claim against the US. In these cases, there would be no duty to disclose information to an owner/operator of a critical infrastructure.[9]

[9] The Department of Health and Human Services, by regulation, limits liability to acts or omissions by government employees only within limited parameters. "With respect to covered individuals, only acts and omissions within the scope of their employment (or contract for services) are covered. If a covered individual is providing services which are not on behalf of the covered entity, such as on a volunteer basis or on behalf of a third-party (except as described in paragraph (d) of this section), whether for pay or otherwise, acts and omissions which are related to such services are not covered." *42 C.F.R. 6.6 (1997)*

For example, E.O. 12812, which provides for the declassification of materials regarding POWs and MIAs, states in Sec. 3: "This order is not intended to create any right or benefit, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person."
E.O. 12951, regarding the release of imagery acquired by space-based reconnaissance systems, contains the same disclaimer.

At this point it is also worth considering the different *notification requirements* in the discussion of the Threat and Hazard Notification Model, *Sections 3 & 4 of Model V,* above. One example (FDA Pesticide Residue) simply calls for the government to send posters to major grocers, excluding smaller grocers (and, more importantly, that sector of the American public which shops at these smaller stores) while the other (CPSC Notification of Banned Hazardous Substances) mandates individual notification by mail of every person who may be affected.

The scope of disclosure required by statute or regulation is relevant. The determining factor in liability under the Tort Claims Act is whether the government agent(s) were negligent in the execution of their duty. If a statute calls for notification of large telecommunications companies, then smaller telecommunications companies may not have a cause of action.

Privacy

Privacy issues are discussed in a separate paper, but should be mentioned here, as they must be taken into account, and applied to each model and cross-model issue as a filter.